ID: 556773
Sample Name: 20c61b30000.dll
Cookbook: default.jbs
Time: 12:54:58
Date: 20/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

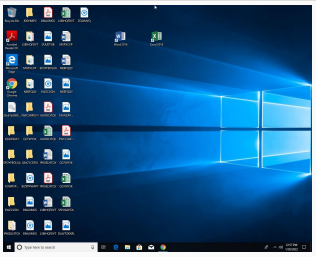
Windows Analysis Report

20c61b30000.dll

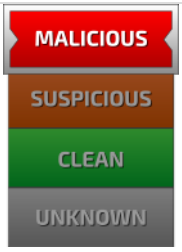
Overview

General Information

Sample Name:	20c61b30000.dll
Analysis ID:	556773
MD5:	11f5556bd5aa4d..
SHA1:	7c5cd9aa98c3dd..
SHA256:	a11f6525353f77e.
Tags:	exe Gozi
Infos:	YARA SIGMA



Detection



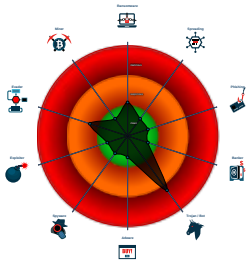
Ursnif

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Sigma detected: Suspicious Call by…
- PE file does not import any functions
- Tries to load missing DLLs
- Program does not show much activi…
- Creates a process in suspended mo…
- Checks if the current process is bei…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7056 cmdline: loaddll64.exe "C:\Users\user\Desktop\20c61b30000.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7088 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\20c61b30000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7132 cmdline: rundll32.exe "C:\Users\user\Desktop\20c61b30000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7120 cmdline: rundll32.exe C:\Users\user\Desktop\20c61b30000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"R+UxqbV/y+ZU1c0seFgwYm43sz1DSmatV8GC7d9ajlQ+vaAx2oxbmrXwev8mSqGGA/bUt2ZkpqSt/nxO6+/Ak7RHUIzazuikwj2CwtI2KIDL8nZsOoWBzTyOzo34t4SghKOmz0ogisuhvhvEfnzRtTwTwtCrGujd4Sa3+qw1BPxaNAN0
DFEVfIrq201z4jAs",
  "c2_domain": [
    "lycos.com",
    "mail.yahoo.com",
    "193.56.255.251",
    "193.56.255.250",
    "193.56.255.249",
    "numolerunosell.online",
    "gumolerunosell.online",
    "rumolerunosell.online"
  ],
  "dga_tld": "com ru org",
  "DGA_count": "10",
  "server": "12",
  "serpent_key": "10291029JSJUYNHG",
  "sleep_time": "60",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "1000",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "122",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "1000",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "122",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "4474",
  "SetWaitableTimer_value": "200"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
20c61b30000.dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Stealing of Sensitive Information

Yara detected Ursnif

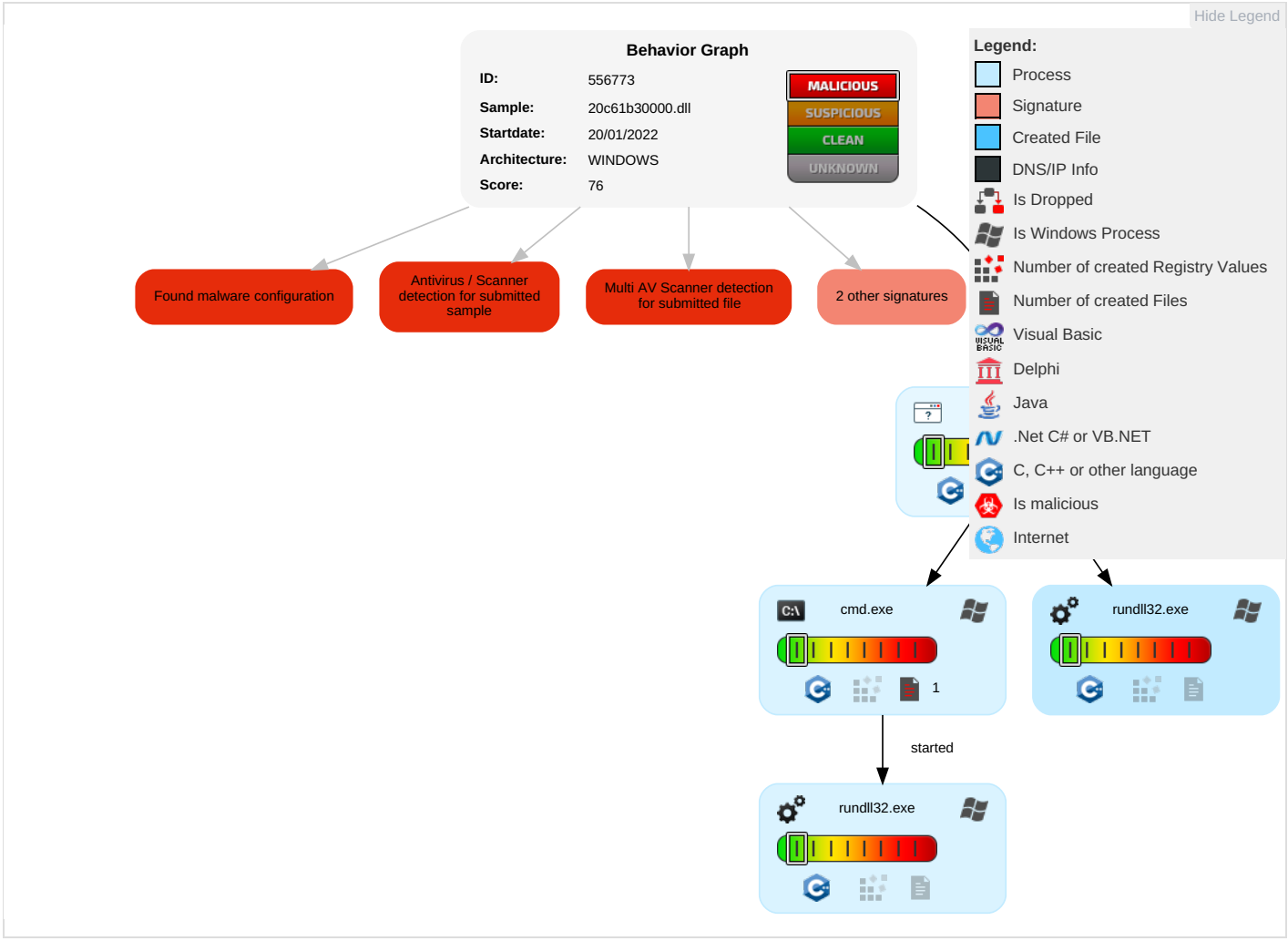
Remote Access Functionality

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Rundll32	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

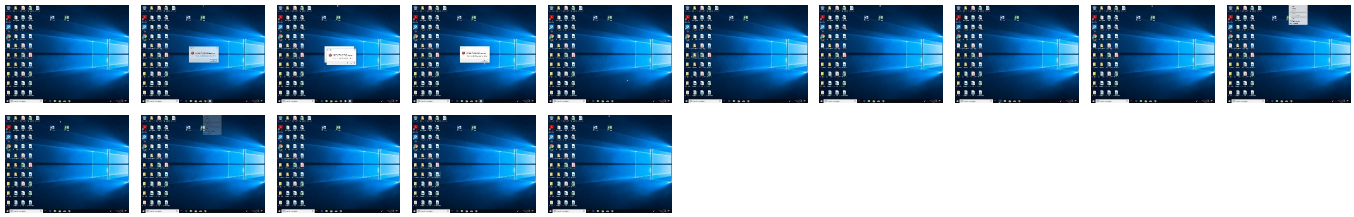
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
20c61b30000.dll	57%	ReversingLabs	Win64.Trojan.Ursnif	
20c61b30000.dll	100%	Avira	HEUR/AGEN.1212258	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	556773
Start date:	20.01.2022
Start time:	12:54:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20c61b30000.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 80.67.82.211, 80.67.82.235
- Excluded domains from analysis (whitelisted): www.bing.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS-DOS executable
Entropy (8bit):	6.40998255347785
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 84.88% • Win64 Executable (generic) (12005/4) 9.99% • DOS Executable Borland Pascal 7.0x (2037/25) 1.69% • Generic Win/DOS Executable (2004/3) 1.67% • DOS Executable Generic (2002/1) 1.67%
File name:	20c61b30000.dll
File size:	227840
MD5:	11f5556bd5aa4dc72e367bd024d7b8c3
SHA1:	7c5cd9aa98c3dd74473687b57cd969acc1d47ce3
SHA256:	a11f6525353f77e4e7a1a25c8884d7ce592f4078d920b21ea012203250e9fe7b
SHA512:	06e30c586c831a6d1ba037fee4637aa3d93c58cad1c19f476d967a289b9d8b503522d74097352ebb87cac178c6a8785c3783a16294355ece41731f6ce7b969fe
SSDEEP:	6144:/HExb7VwvtKNbnvSxYNiyf+D3Luiy56H:cxb5wvtKRvSxY0G+D7uij
File Content Preview:	MZ.....PE..d..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18002a0e8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x60C0F8C1 [Wed Jun 9 17:22:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	

Entrypoint Preview

Instruction
inc eax
push ebx
dec eax
sub esp, 20h
mov ebx, 00000001h
test edx, edx
je 00007FE130A5CC26h
cmp edx, ebx
jne 00007FE130A5CC31h
mov eax, ebx
lock xadd dword ptr [0000A8ABh], eax
add eax, ebx
cmp eax, ebx
jne 00007FE130A5CC21h
dec ecx
mov edx, eax
call 00007FE130A3A24Eh
test eax, eax
je 00007FE130A5CC15h
xor ebx, ebx
jmp 00007FE130A5CC11h
lock add dword ptr [0000A88Dh], FFFFFFFFh
jne 00007FE130A5CC07h
call 00007FE130A4E74Fh
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
jmp dword ptr [00004228h]
dec esp
mov ebx, esp
push ebx
push ebp
push esi
push edi
inc ecx

Instruction
push esp
dec eax
sub esp, 60h
dec ecx
lea eax, dword ptr [ebx-50h]
dec esp
lea esp, dword ptr [FFFD5EB0h]
dec ebp
lea eax, dword ptr [ebx-50h]
dec ecx
mov dword ptr [ebx-48h], eax
dec ecx
lea eax, dword ptr [ebx-50h]
xor edi, edi
dec ecx
mov dword ptr [ebx-50h], eax
dec eax
mov eax, dword ptr [0000AA37h]
inc ebp
xor ecx, ecx
dec edx
lea edx, dword ptr [eax+00038468h]
dec edx
lea ecx, dword ptr [eax+00037750h]
mov dword ptr [esp+28h], 00000001h
mov dword ptr [esp+20h], edi
call 00007FE130A5C074h
cmp eax, edi
je 00007FE130A5CC9Ah
dec eax
mov ebx, dword ptr [esp+38h]
dec esp
lea eax, dword ptr [esp+000000A0h]
dec eax
lea edx, dword ptr [esp+30h]
dec eax
lea ecx, dword ptr [ebx+28h]
dec eax
mov esi, ebx
call 00007FE130A5CC92h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x32ad0	0x37	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x31a70	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x35000	0x17c4	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3a000	0x330	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2e000	0x508	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x2fdf8	0x1e0	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

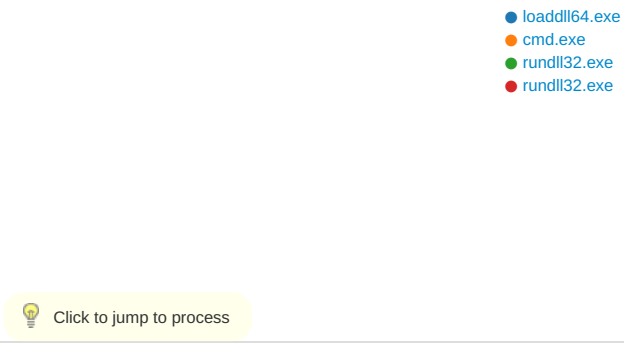
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2c908	0x2ca00	False	0.57014290091	data	6.34156774345	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2e000	0x4b07	0x4c00	False	0.399362664474	data	5.24927821467	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x33000	0x1f88	0x1a00	False	0.307542067308	lif file	3.70326717279	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x35000	0x17c4	0x1800	False	0.538411458333	data	5.29492234825	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x37000	0x20c8	0x2200	False	0.952895220588	data	7.87054877548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3a000	0x1000	0xc00	False	0.459635416667	data	4.35925404581	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 7056, Parent PID: 5268

General

Start time:	12:55:58
Start date:	20/01/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\20c61b30000.dll"
Imagebase:	0x7ff6f3970000
File size:	140288 bytes

MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 7088, Parent PID: 7056

General

Start time:	12:55:59
Start date:	20/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\20c61b30000.dll",#1
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7120, Parent PID: 7056

General

Start time:	12:55:59
Start date:	20/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\20c61b30000.dll,#1
Imagebase:	0x7ff6a0c30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7132, Parent PID: 7088

General

Start time:	12:55:59
Start date:	20/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\20c61b30000.dll",#1
Imagebase:	0x7ff6a0c30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly